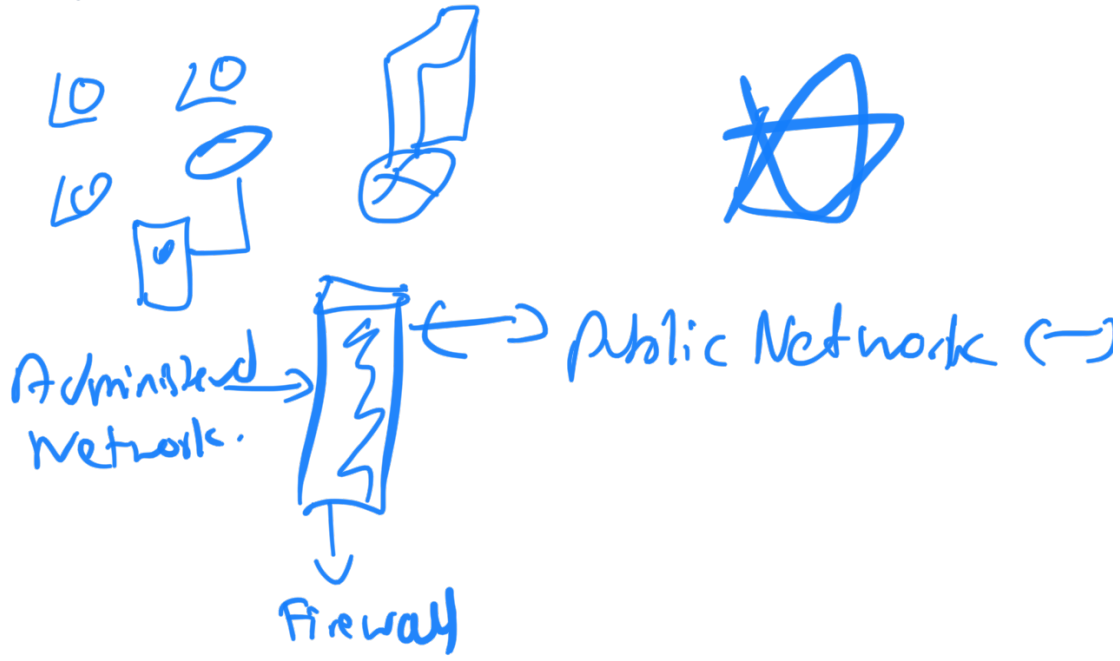
Week 4

Firewalls.

Firewall isolates organization's internal net from larger internet, allowing some packets to pass, blocking others



Firewalls: Why -

→ prevent denial of service attacks
→ prevent illegal modification/access of internal data

→ allow only authorized access to inside network.
→ two types of firewalls:
  → application-levels
  → packet-filtering.

Packet Filtering.

→ internal network connected to Internet via router firewall
→ router filters packet-by-packet, deciding to forward/drop packet based on:
  → source IP address, destination address
  → TCP/UDP
  → ICMP
  → TCP SYN and ACK bits.

Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.

So, All incoming and outgoing UDP flows and telnet connections are blocked.

Example 2: Block inbound TCP segments with ACK=0.

So, this prevents external clients from making TCP connection with internal clients.

Application Firewall Gateway.

↳ Filter Packets. IP/UDP/TCP

Ex. allows select internal users to telnet outside.

Limitations of firewall and gateways.

→ IP Spoofing: router can't know if data is claimed save.

→ If multiple apps needs special treatment: SD IP smart.

Firewalls – XML Gateway.

↳ XML traffic passes through a conventional firewall without inspection.

↳ XML gateway of the XML examining the payload message.

Firewalls → stateless and stateful

→ Filter traffic between networks.
→ Handle packets differently
→ Multi-NICs connected.

Stateless Firewall → → no concept of 'state'

↓

less secure

→ Also called Packet Filter.

→ Filters packets based on Layer 3 and 4 information (IP and port)

→ Lack of state makes it less secure.

Stateful Firewall

→ Have state tables that allow the firewall to compare current packets with previous packets.

→ Could be slower than packet filters but can more secure.

→ Application firewall can make decisions based on Layer 7 and information.

Antivirus / Anti-malware.

→ Specialized software that can detect, prevent and even destroy a computer virus or malware

→ Uses malware definitions
→ Scans the systems and searches for matches against the malware definitions.
→ These definitions get constantly updated by vendors.

Introduction to Cryptography.

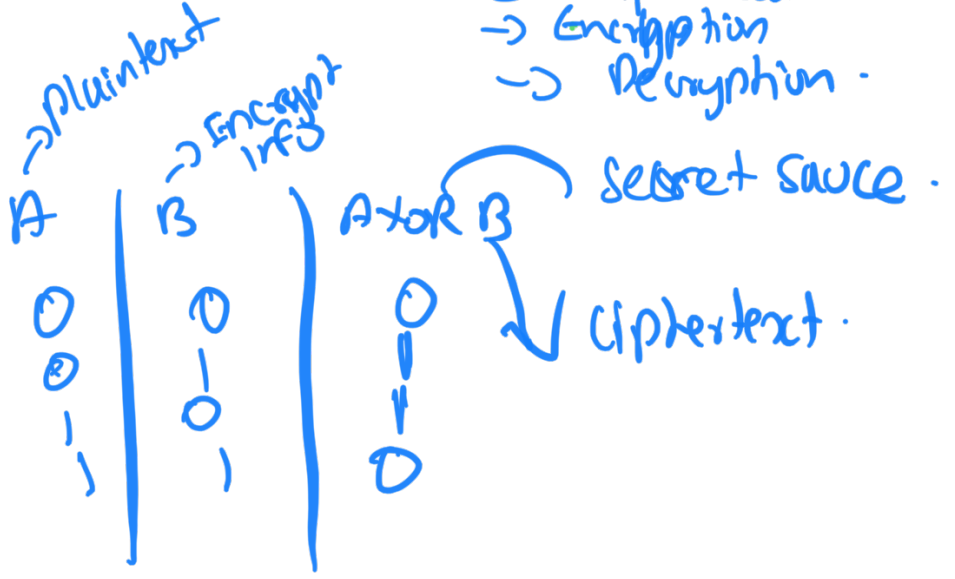
Cryptography

- Is secret writing.
→ Secure communication → that might be only understood by the intended recipient only
→ It's been used for 1000 years

→ Egyptians Hieroglyphics, Spartan Scytale, Ceaser Cipher → ancient cryptography.

Key concepts. → Confidentiality

→ Integrity
→ Authenticity
→ Non-repudiation
→ Cryptoanalysis
→ Cryptology
→ plaintext
→ Ciphertext
→ Encryption
→ Decryption.



Types of Symmetric Encryption.

1. Symmetric Encryption:
   - → use the same key to encrypt and decrypt.
   - → security depends on keeping the key secret at all times
   - → Strengths include speed and Strenght of every key.

Ex. DES, Triple DES,
- → the bigger the key → the stronger the algorithms.

AES
- → out of band method.

2) Asymmetric Encryption.

→ Uses two keys.
→ One key public and other private.
→ One for encryption and other for decryption.
→ PKI → Public Key infrastructure.
→ "One way" algorithm to generate that two keys. Like factoring prime numbers, one discrete logarithm.
→ slower than symmetric encryption.

3.) Hash Function.

→ provides encryption using an algorithm and no key
→ plaintext is hashed
→ Integrity verification
→ SHA1, MD5, older hash alg
→ SHA2 → newer and recommended algorithm.

Cryptographic Attacks.

1.) Brute Force (trial & error)
2.) Rainbow Tables
3.) Social Engineering
4.) Known Plaintext
5.) Known Ciphertext.

First look at Penetration Security and Digital Forensics.

Pentesting is the practice of testing computer system, network, or applications to find security vulnerabilities that an attacker could exploit.

Hackers

White Hat
- ethical Hackers
  → work done under contract for security Reasons.

Grey Hat
→ Between White & Black.
→ look for vulnerabilities in a unauthorized manner and report back to victim.

Black Hat
→ Do it for personal recognit
→ Bad Guys

Threat Actors
→ An entity that is partially or Wholly responsible for an incident that affects or potentially affects an organization's security.

Vulnerability Tests.
1. Identify
2. Exposure
3. Sensitivity
4. potential impacts
5. Adaptive capacity

Indicators

Vulnerabilities

What is Digital Forensics.
→ Branch of Forensic Science.
→ Chain of custody.

Tools → Volatility.
FTK
Encase
→ dd
→ Autopsy.